REMARKS

In an Office Action dated June 3, 2005, the Examiner rejected claims 10-16, 18-26, 28-35, 44-49, 51-55, 97-115 and 117-126 under 35 U.S.C. 102(b) as anticipated by Fischer (U.S. Patent 4,868,877), and rejected claims 17, 27, 36, 37-43, 50 116 and 127 under 35 U.S.C. 103(a) as unpatentable over *Fischer* in view of Naccache (U.S. Patent 5,910,989).

Outstanding Restriction

In response to the previous office action, applicants partially traversed the restriction requirement and provisionally elected claim Group II. The Examiner has examined claim Group II and issued the current action on the merits, without explicitly responding to applicants' partial traverse or stating that the restriction requirement is final. Applicants have therefore assumed that the restriction requirement is final, and have cancelled non-elected claims. Applicants respectfully request that the Examiner confirm applicants' understanding. Applicants reserve the right to re-assert any claims which are added to Group II in the event the Examiner changes the claim groupings.

Claim Amendments

Claims 51-55 have been cancelled, and the rejections thereof are moot. Applicants have amended the remaining independent claims to clarify certain matters, particularly the nature of an object being protected and the relationship between the data protection mechanism and the object. As amended, the claims are patentable over the cited art.

Independent claims 10, 20, 28, 37 and 44 have been amended to clarify that the digital protection system is a tangible device which is physically attached to the tangible object, and which is itself a data processing device which processes data independently of the tangible object. In the general case, the tangible object being protected is not necessarily a data processing device,

although it could be such a device. But even if the tangible object is itself a data processing device, the recited "digital protection system" is a tangible device operating independently, which in the preferred embodiment is a so-called smart chip. Thus the "digital protection system" and the protected "tangible object" are not one and the same data processing system, and the tangible object is emphatically not data.

Independent claims 97, 106 and 117 have similarly been amended to recite that the recited "carrier" or "digital personal identity document" is a portable tangible device, which is carried by a person to whom it relates. As in the case of amendments to the other independent claims, these amendments clarify that the "carrier" or "document" is not data floating around a network.

Independent claim 28 has been further amended to recite additionally that the request to update attribute data includes the old data and digital signature, and that these are verified by the service provider.

Although perhaps unnecessary, applicants have further amended independent claims 97, 106 and 117 to replace the term "subject" with "natural person". Applicants believe it was already clear from the context that "subject" was a natural person, but applicants wish to avoid any possible ambiguity or argument that "subject" might include other things, like data objects. Various dependent claims have also been amended to use consistent language.

Applicants have added new claims 141-151. New claims 141 and 142 are dependent on claims 28 and 97, respectively. New claim 143 is independent, and is similar to claim 10 except that it explicitly recites that the tangible object is something other than a data processing device. As such, independent claim 143 does not necessarily read on all of the exemplary embodiments disclosed in applicants' specification, although it does read on some (such as a passport). New claims 144-151 are dependent on new claim 143.

Invention Overview

Applicants' invention is directed to the protection or verification of ***tangible objects***, including people. It should be borne in mind that, in general, prior art techniques in this field have not necessarily involved data processing or data encryption at all, but have involved methods which attach physical identifying marks to the tangible object, in such a way that alteration is likely to be detected. For example, serial numbers might be stamped on a metal part; paper identity documents include special paper, watermarks, special inks and so forth which make forgery difficult, and so forth.

At the same time, various encryption methods have existed in the prior art for protecting data. Public/private key encryption algorithms have also been applied to the authentication of electronic data received from a remote source. These authentication techniques are commonly known as digital signatures. A digital signature is a form of backward encryption, in which unencrypted data is sent along with a "decrypted" version of the data derived by applying a private key (the "digital signature"). Typically, the raw data is hashed before decryption to reduce its size, although this is not strictly required. The signature is then "encrypted" with the public key and compared with the raw data (or hashed version thereof) to verify the authenticity of the data.

Applicants do not claim to have invented public/private key encryption algorithms or digital signatures. But it is important to remember that digital signatures were designed to verify ***data*** received from remote sources. What applicant's claim to have invented is a technique for verifying or authenticating ***tangible objects*** (including people) using these existing tools. Applicants therefore use certain basic building blocks of conventional remote electronic transaction technology to build an entirely new and unobvious combination which is used to solve a completely different family of problems.

Anticipation

Applicants will address the obviousness rejection presently, but first address anticipation. The independent claims are not anticipated by *Fischer* because, among other things, all independent claims recite a protected "tangible object" (or carrier for a personal identity document) to which a tangible data processing device is attached. Fisher's protected "object" is just data.

Fischer discloses a public/private key system for verifying digital electronic transactions. In accordance with *Fischer*, an originator of an electronic message includes the message data itself, a certificate specifying a public key, and a digital signature comprising an "decrypted" hash of the data and public key using the private key. The thrust of *Fischer*'s technique appears to be that the certificate may further include data concerning its use, such as the authority granted to the party be certified, whether co-signatures are required, and so forth. The recipient of the message "encrypts" the signature using the public key, and compares it to the a hash of the data using the same hashing function to verify the data contents.

The Examiner's rejection, as nearly as applicants can understand it, equates *Fischer*'s "object" (feature 20) with the tangible object recited by applicants. Leaving aside all other claim recitations which are not met, there is nothing whatsoever in *Fischer* which teaches or suggests that the "object" which is the subject of its digital certification technique might be anything other than data. *Fischer* is directed to the verification of data received from remote sources, consistent with the conventional use of digital signature technology. The example given by *Fischer* is a purchase order, and in the context of *Fischer*, this is a purchase order in the form of an electronic transaction, i.e. data. *Fischer*'s "object" is not a tangible object at all, and for that reason alone, irrespective of any other lack of critical elements, *Fischer* does not anticipate the independent claims herein.

Obviousness[1]

The Examiner further rejected certain claims as obvious over *Fischer* and *Naccache*. *Naccache* is cited to show the technique of generating random data as a method of testing a correspondence between a public and a private key of a public/private key pair, and it directed particularly to a method involving reduced computations which can be implemented by small microprocessors.

As explained above, the use of digital signatures and public/private key encryption is well known in the art of electronic transactions. But these techniques were designed specifically for facilitating the electronic transfer of data and conducting of business with remotely located data processing systems. These techniques were not conceived and designed for the purpose of protecting and authenticating tangible objects.

There are many situations in which it is desirable to authenticate a tangible object and information about that object, and many possible ways to do so, some more sophisticated than others. As explained previously, many prior art techniques are directed to visual markings on the object, which are difficult to counterfeit. Efforts to invent new and more successful techniques of this sort abound, and there is little doubt that improvements in this field will continue to be made.

Applicants' invention is directed to a certain subclass of these situations, in which it is generally desirable that the tangible object carry a significant amount of information, that the information be immune to forgery, and that the object be able to authenticate itself. In some of these situations, it is further desirable to be able to update the information in a secure manner.

---

[1] The rejection of the independent claims as anticipated by *Fischer* carries a subsumed rejection as obvious over *Fischer*, which is addressed here.

The ability to authenticate itself is important because it is expected that the tangible objects being protected will be larger in number, will be scattered in diverse locations, and will often be mobile or poratble. It is not generally practical to have the tangible object physically examined by someone capable of making the judgment of authenticity (or, in the case of a personal identity document, having the person in question so examined).

In accordance with the preferred embodiment of applicant's invention, the problem of self-authentication is solved by using two separate public/private key pairs. The first pair, an identity key pair, is used to test the digital protection system (e.g. smart chip) physically attached to the tangible object, by a two-step encryption/decryption of random data. The second pair, a signature key pair, is used to verify the digital signature, which in turn verifies both the identity public key and the attribute data about the object. The use of both pairs provides a high degree of protection against copying and alteration. The use of the identity key pair alone could verify that the identity public key matches the identity private key of the tangible object, but if the verifier does not itself know the public key, there is no way of knowing whether the identity public key itself is correct (without reference to some external authority). The use of a signature key pair alone could protect attribute data, but it could not protect against simple duplication of the attribute data and signature key..

The Examiner may point out that the broadest independent claims doesn't recite the use of a second pair of public/private keys, called a signature key pair, to verify the attribute data and identity public key. This is true, but all claims recite at least that the attribute data and identity public key are verified. It is applicant's disclosure which teaches an easily implementable and secure technique for verifying the attribute data and identity public, key, i.e., by using the second key pair. Because the prior art does not disclose *any* such technique, applicants are entitled to broadly claim a method in which the attribute data and identity public key are verified, without restriction as to technique. Furthermore, many of the claims explicitly recite the use of a second

pair of public/private keys (specifically, independent claim 37 and dependent claims 11, 21, 29, 30, 47, 103, 113, and 118, as well as new claim 144).

Thus, in hindsight it can be seen that applicants' invention achieves something analogous to what is achieved by a certification authority in the field of electronic transactions. ***But there is no such certification authority for protecting tangible objects.*** Applicant has effectively applied ideas designed for use in remote electronic transactions to an entirely new field.

It is all too easy to find, in hindsight, the various elements of an invention from the prior art, or to ask what difference it makes whether these elements are used for authenticating remote electronic messages or tangible objects. But the prior art systems were designed specifically for the purpose of verifying remote electronic transactions. It was for this purpose that certification authorities were created. There is nothing in *Fischer*, nor indeed in any other cited art, which would suggest the combination disclosed and claimed by applicants for the protection and verification of tangible objects. The suggestion to create such a combination came from only one place: applicants' disclosure. For all of the above reasons, the independent claims herein are patentable over the cited art.

Applicants further submit that various claims herein recite additional features which, in addition to the reasons stated above, establish novelty and non-obviousness. The claimed feature of a second pair of keys (the signature pair) has been discussed above. In addition to these claims, certain specific such claims are identified below.

Claims 97-127 and 142 (independent claims 97, 106 and 117) recite a personal identity document, such as a passport, an apparatus for verifying such a document, or a method for verifying it. All of these claims recite that the document is a portable device for accompanying the person to whom it relates, and the document itself contains personal attribute data which can

be verified. This is a specific application of the technique claimed more generally in certain other independent claims. The verification of such personal identity and attribute information in a secure manner is a matter of utmost importance in this day and age. In general, it must be assumed that such a document will be carried to diverse parts of the world, and that an attempted forgery (either by copying an existing document, altering such a document, or creating an entirely new such document) might occur anywhere. Applicants' technique provides a high degree of security for considerable information (including biometrics) of the subject, making unauthorized tampering very difficult. There is nothing in *Fischer* or *Naccache* which would suggest this particular application, or the way in which it is achieved.

Independent claims 44, 97, 106 and 117, as well as dependent claims 16, 26, 141, 40, and 149, recite that the descriptor data is obtained from the digital protection device itself. In the preferred embodiment, this is an important aspect of self-authentication, which supports portability of the tangible object and verification in non-secure environments. *Fischer* does show that a public key and digital signature accompany an electronic message, but the environment is much more controlled, and the public key includes a certificate from a certifying authority. *Fischer* does not teach or suggest, alone or in combination with *Naccache*, the obtaining of descriptor data from a tangible object itself to be verified.

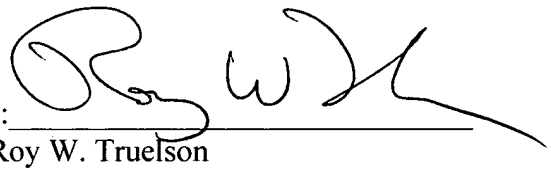
Claims 28-36 and 141 recite a method for updating attribute information, which is amenable to being done via a remote server, in which the old information is transmitted and verified, the identity of the requestor is verified, and a new descriptor is generated by the server. Claims 33 and 34 recite specifically that this procedure is performed remotely from the tangible object. *Fischer* discloses how electronic messages are created, and *Naccache* discloses verification of a key in a smart card, but the problem of updating information in a tangible object, which is not necessarily in a secure location, is a novel one and is not addressed at all by *Fischer* or *Naccache*.

For all of the reasons stated above, the claims, as amended, are neither anticipated by nor obvious over the art cited herein.

In view of the foregoing, applicants submit that the claims are now in condition for allowance and respectfully request reconsideration and allowance of all claims. In addition, the Examiner is encouraged to contact applicants' attorney by telephone if there are outstanding issues left to be resolved to place this case in condition for allowance.

Respectfully submitted,

DAVID O. LEWIS, et al.

By: 

Roy W. Truelson
Registration No. 34,265

Telephone: (507) 202-8725